INDICATEURS DE SECURITE

Juillet 2001

Version 1.0

Commission Méthodes

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30 rue Pierre Sémard – 75009 PARIS
Téléphone : 01 53 25 08 80 Fax : 01 53 25 08 88
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

Le CLUSIF

Le CLUSIF, fondé en 1984, offre un cadre dans lequel les acteurs de la sécurité des systèmes d'information peuvent se rencontrer, échanger leurs points de vue, travailler et progresser ensemble. A ce jour, le CLUSIF rassemble plus de 430 membres, appartenant à 250 organismes ou sociétés. Sa particularité est d'accueillir aussi bien les utilisateurs que les offreurs, fondant sa culture sur une égale participation des uns et des autres et son dynamisme sur une confrontation permanente de l'offre et de la demande.

Nos missions

Echanger

Favoriser activement les échanges entre membres offreurs et utilisateurs :

- Pour qu'ils puissent partager leurs expériences
- Pour que les utilisateurs soient tenus au courant des nouveautés en matière de sécurité
- Pour que les offreurs aient une meilleure connaissance des besoins et du marché

Concevoir

La conception de travaux sur la sécurité couvre : des travaux de recherche et développement, des prises de position sur des sujets d'actualité, des guides et recommandations à caractère didactique, l'état de l'art sur différents types de solutions, des méthodes (analyse des risques, conception et développement sécurisés de projets, évaluation de la sécurité des systèmes d'information), des enquêtes, des statistiques, des recueils de cas de sinistres, des outils de sensibilisation.

Promouvoir

Il entre dans les finalités du CLUSIF d'influencer un certain nombre d'acteurs de la sécurité, avec le double objectif de promouvoir la sécurité et faire valoir les besoins et contraintes des utilisateurs auprès des instances dirigeantes. Les cibles visées sont les décideurs, les utilisateurs, les parlementaires, les pouvoirs publics, les autres associations, les médias, le public.

Eduquer

Le CLUSIF s'implique activement dans le processus éducatif et de sensibilisation auprès des membres (en particulier par les séances thématiques), des professionnels de la sécurité des enseignants et des étudiants. Le CLUSIF intervient par : son implication dans les programmes de formation, des actions vis-à-vis du système éducatif pour que la sécurité des systèmes d'information soit incorporée dans les programmes pédagogiques.

Fonctionnement

Le mode principal de fonctionnement du CLUSIF est le travail en commission. Cependant, de plus en plus, des groupes de travail temporaires sont créés afin de produire un document, un guide, une recommandation, ou une simple prise de position sur un thème donné.

Commissions

- Espace RSSI
- Évaluation
- Menaces
- Méthodes
- Micro-informatique
- Réseaux et systèmes ouverts
- Technique de sécurité logique
- Technique de sécurité physique

Comités

L'orientation, le contrôle et l'animation des diverses activités du CLUSIF se font à travers des comités spécialisés :

- Droit et Assurance
- Éthique

Réseau de relations

Régions

Le CLUSIF dispose de relais dans les régions au travers des Clubs de la Sécurité des Systèmes d'Information Régionaux (CLUSIR). Ces associations indépendantes sont agréées par le CLUSIF et s'engagent à respecter le règlement intérieur et le code éthique du CLUSIF. Il existe à ce jour sept CLUSIR : **Est** (Strasbourg), **Languedoc Roussillon** (Montpellier), **Midi-Pyrénées** (Toulouse), **Normandie** (Rouen), **Provence-Alpes-Côte-d'Azur** (Marseille), **Pays de Loire** (Nantes), **Rhône-Alpes** (Lyon).

Nations

Le CLUSIF entretient des contacts avec des associations ou organismes en Afrique du Sud, en Allemagne, en Argentine, en Belgique, en Italie, au Luxembourg, au Maroc, au Québec, en Suisse et en Tunisie.

Associations

Le CLUSIF entretient des relations avec des organismes proches qui partagent le même souci de la Sécurité Informatique dont les principaux sont :

AFAI (Association Française d'Audit et du conseil en informatique) ;

AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) ;

CIGREF (Club Informatique des Grandes Entreprises Françaises) ;

Forum des Compétences (club de Responsables de la Sécurité d'organismes bancaires).

Contact

Pour toute information, vous pouvez contacter le :

Secrétariat du CLUSIF
30 rue Pierre Sémard
75009 Paris
Tel : 01 53 25 08 80 - Fax : 01 53 25 08 88
Courrier électronique : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Commission Méthodes

Contexte

En raison de l'évolution des systèmes d'information, les méthodes existantes d'analyse et de management de la sécurité ont nécessité une adaptation aux besoins des RSSI et des auditeurs. La commission Méthodes s'est créée, en 1992, autour d'experts qui ont eux-mêmes participé à l'élaboration des premières méthodes françaises MARION et MELISA. La richesse de ces cultures a permis le développement d'une méthode prenant en compte le domaine de l'informatique distribuée par un découpage cellulaire de l'entreprise à travers MEHARI.

Objectifs

La commission Méthodes a pour but de proposer de nouvelles réflexions sur la gestion des risques informatiques en entreprise, notamment à l'aide de la méthode MEHARI.

Travaux

Les travaux de la commission et de ses groupes de réflexion concernent pour une part les évolutions de la méthode MEHARI (mise à jour des bases de connaissance, rédaction d'un didacticiel…), mais aussi des travaux plus généraux de gestion des risques, tels qu'une recherche de modélisation de l'induction des risques ou la constitution d'un recueil d'indicateurs de suivi de la sécurité.

Pour améliorer la pertinence des bases de connaissance et des questionnaires, la commission travaille en collaboration avec d'autres commissions du CLUSIF, telles que :

- Techniques de sécurité physique
- Techniques de sécurité logique
- Réseaux et systèmes ouverts
- Sécurité et Qualité

Projets

La commission Méthodes prévoit d'assurer :

- la pérennité des méthodes développées par le CLUSIF
- la mise à jour des questionnaires et des bases de connaissances

Publications

La commission a publié :

- le questionnaire MARION et ses déclinaisons (MARION-PMS, MARION-Micro) ;
- la démarche MEHARI et ses bases de connaissances (questionnaire d'audit rapide, scénarios, services de sécurité, questionnaire d'audit par service de sécurité) ;
- la démarche de conception d'un Tableau de Bord ;
- un document de synthèse présentant les méthodes de management des risques du Clusif ;
- un recueil d'indicateurs de suivi de la sécurité.

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document :

Jacques	**BOUSTANI**	New Tech Informatique
Dominique	**BUC**	BUC S.A.
Marie-Hélène	**COURBIS**	New Tech Informatique
Annie	**DUPONT**	JAA
Jean-Philippe	**JOUAS**	2SI
Gérard	**MOLINES**	Molines Consultants

Table des matières

1 INTRODUCTION 1
1.1 Des indicateurs pour aider qui ? 1
1.2 Objectifs des indicateurs 1
1.3 Dynamique des indicateurs 2
1.4 Construire des indicateurs à l'aide de la méthode MEHARI 3
1.5 Indicateurs simples ou composés 3
2 EXEMPLE D'INDICATEURS DE SECURITE PAR DOMAINE 5
2.1 Sécurité liée à l'organisation 7
2.2 Sécurité liée au site et à l'établissement 9
2.3 Protection des locaux 11
2.4 Sécurité des architectures réseaux et télécommunications 13
2.5 Exploitation des réseaux et télécommunications 15
2.6 Sécurité des systèmes et de leur architecture 17
2.7 Production Informatique 19
2.8 Sécurité applicative 21
2.9 Sécurité des projets et développements 23

1 Introduction

Un indicateur est une **donnée objective** qui décrit une **situation** du strict point de vue **qualitatif** et qui **constate un résultat**.

1.1 Des indicateurs pour aider qui ?

- Le Responsable de la Sécurité des Systèmes d'Information (R.S.S.I.) qui assure le niveau de sécurité des systèmes d'information de l'entreprise.
- La Direction Générale qui définit une stratégie de sécurité conforme aux enjeux de l'entreprise.
- Les Conseils d'administration, les Comités (ou Conseils) de surveillance des entreprises cotées ou non en Bourse.
- Le Consultant Sécurité (ou société de conseil) intervenant dans une entreprise utilisant la méthode MÉHARI ou tout autre moyen d'audit ou d'investigation.

1.2 Objectifs des indicateurs

Les objectifs des indicateurs, regroupés sous forme de « tableau de bord », sont :

- suivre la **qualité des services de sécurité**,
- suivre la **qualité de la politique de sécurité** établie,
- remonter les **alertes** afin de **prévenir les dysfonctionnements**,
- fournir un outil synthétique d'aide au système d'assurance et de gestion de la sécurité.

Les contraintes du tableau de bord sont :

- Devoir véhiculer seulement les informations **pertinentes**.
- Devoir comporter un **nombre très limité** d'indicateurs.
- Nécessiter de vérifier **la pertinence des éléments** ou événements à mesurer.
- Nécessiter de **déterminer les valeurs cibles à atteindre** ainsi que leur **seuil de tolérance**.
- Nécessiter d'adapter une **fréquence adaptée à une exploitation attentive**.

Les indicateurs décrits dans les pages suivantes **ne sont pas exhaustifs** mais peuvent être **pertinents** pour l'entreprise si les seuils sont adaptés.

1.3 Dynamique des indicateurs

Tandis que la politique de la sécurité est communiquée de haut en bas, les indicateurs sont communiqués du bas vers le haut.

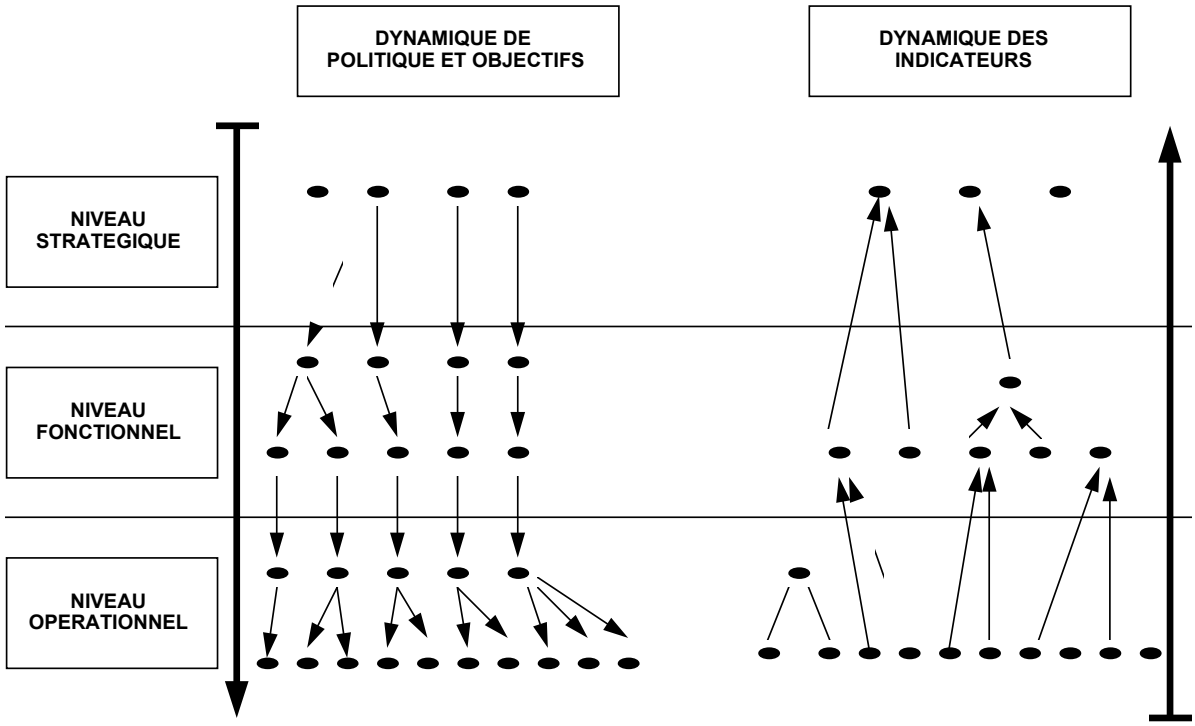

Figure 1 : Dynamique des indicateurs.

INDICATEURS STRATEGIQUES :	Plusieurs indicateurs stratégiques peuvent alimenter un indicateur Stratégique Un indicateur stratégique peut être indépendant.
INDICATEURS FONCTIONNELS :	Plusieurs indicateurs fonctionnels peuvent alimenter un indicateur stratégique Plusieurs indicateurs fonctionnels peuvent alimenter un indicateur fonctionnel Un indicateur fonctionnel peut être indépendant.
INDICATEURS OPERATIONNELS :	Plusieurs indicateurs opérationnels peuvent alimenter un indicateur opérationnel Plusieurs indicateurs opérationnels peuvent alimenter un indicateur fonctionnel Un indicateur opérationnel peut être indépendant.

1.4 Construire des indicateurs à l'aide de la méthode MEHARI

Des indicateurs peuvent qualifier les scénarios de sinistre spécialement étudiés et issus de la méthode MEHARI, à l'intérieur d'une unité opérationnelle ou globalement au niveau de l'entreprise.

A partir de la méthode MÉHARI, les indicateurs peuvent s'appliquer à d'autres contextes, notamment pour la surveillance de certains risques précis.

1.5 Indicateurs simples ou composés

Il existe deux types d'indicateurs de mesure : les **indicateurs simples** et les **indicateurs composés**.

Un indicateur simple comporte :

- une question ;
- une pondération ;
- un ensemble de valeurs de référence ;
- une procédure.

Un indicateur composé comporte, en plus des éléments de l'indicateur simple, un ou plusieurs opérateurs et/ou un indicateur de comparaison.

2 Exemple d'indicateurs de sécurité par domaine

2.1 Sécurité liée à l'organisation

	Services	Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
01A	**Rôle et structure de la sécurité**				
	Les indicateurs doivent refléter le rôle et la structure de la sécurité. Ils mesureront par exemple :				
	période				
	Nbre de correspondants sécurité du SI / Nbre d'entités ou de services dans l'entreprise				
01B	**Sensibilisation et formation à la sécurité**				
	Les indicateurs doivent refléter l'évolution de la sensibilisation de l'entreprise et la formation du personnel à la la sécurité, l'évolution du règlement intérieur et de la politique de sécurité,la vie des ressources de l'entreprise, l'évolution des rel				
	Dates des dernières formations				
	Taux de renouvellement des formations				
	Taux d'exercices d'évacuation au cours de la période				
	Taux de personnel formé à la sécurité incendie				
	Taux d'infractions par rapport aux procédures définies				
	Taux d'audits effectués au cours de la période				
	Date de la dernière mise à jour du règlement intérieur				
	Taux de clauses de confidentialité signées				
	Taux de ressources ou de documents classés				
	Taux de ressources matérielles classifiées / nombre de ressources matérielles installées				
	Nombre de contrats visés par le service juridique / Nombre de contrats signés avec les fournisseurs (pour un montant > à x kF)				
	Dates des dernières révisions des contrats d'assurance				
	Nombre de contrats d'assurance révisés / nombre total de contrats d'assurance				
	Date de la dernière mise à jour des déclarations à la CNIL				
01C	**Gestion des ressources humaines**				
	Les indicateurs doivent refléter la criticité des ressources humaines pour les postes stragégiques ou sensibles, l'évolution des responsabilités, l'adaptabilité du suivi des incidents, etc.				
	Taux de jours en situation critique (moins de deux personnes dans un domaine)				
	Taux d'intérimaires engagés sur la période pour assurer des postes sensibles				
	Taux d'absentéisme sur la période (pour les postes sensibles)				
	Taux de remplacement des postes sensibles sur la période				
	Nombre de propriétaires d'informations désignés / Nombre de services dans l'entreprise				
	Evolution du nombre (ou taux) d'incidents enregistrés sur la dernière période				
	Evolution de l'impact des incidents sur la dernière période				
	Nombre de nouveaux incidents (non déjà répertoriés) sur la période				
01D	**Assurances**				
	Les indicateurs doivent refléter la présence et l'évolution des contrats d'assurances				
	Nombre de polices d'assurances				
	Nombre d'avenants par type de polices d'assurances				
	Date de dernière mise à jour par type de polices d'assurances				

2.2 Sécurité liée au site et à l'établissement

	Services	Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
02A	**Implantation du site**				
	Les indicateurs doivent refléter l'évolution des risques de type accidentel ou d'environnement				
	Evolution des menances naturelles (innondations, sismiques, climatiques, etc.)				
	Evolution des menaces industrielles (pollution, etc.)				
	Evolution du taux de vandalisme dans la région d'implantation				
	Nombre d'actions terroristes recensées dans la région d'implantation au cours de la période				
02B	**Contrôle d'accès au site**				
	Les indicateurs doivent refléter la fréquentation et la diversité des populations accèdant au site				
	Nombre d'incidents détectés au cours de la période				
	Nombre d'incidents détectés / nombre de patrouilles effectuées				
	Nombre d'incidents détectés par catégorie de population (ouvriers, employés, cadres, extérieurs, etc.)				
02C	**Contrôle de la circulation sur le site**				
	Les indicateurs doivent refléter les incidents liés à la circulation tant du personnel interne qu'externe, à la circulation des visiteurs qu'aux fournisseurs, etc.				
	Nombre de déclaration de perte de badges au cours de la période				
	Nombre de visiteurs interceptés sans possession de badge				
	Nombre d'effractions constatées au cours de la période				
02D	**Gestion de la sécurité physique**				
	Les indicateurs doivent refléter le niveau des failles dans le système de sécurité physique				
	Evolution de la protection des enceintes du site				
	Evolution de l'état des toitures				
	Nombre de fuites détectées au cours de la période				
	Evolution du fonctionnement des sas d'entrée par sas au cours de la période				
	Nombre d'interventions des Hommes de l'art sur le site au cours de la période				

2.3 Protection des locaux

Services		Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
03A	**Services généraux**				
	Les indicateurs doivent refléter l'évolution de la qualité de la fourniture des services				
	Taux de disponibilité de l'électricité				
	Taux de disponibilité de la climatisation				
03B	**Contrôle d'accès aux bâtiments contenant les locaux sensibles**				
	Les indicateurs doivent refléter l'évolution de la qualité du contrôle d'accès				
	Nombre de personnes autorisées à circuler dans les locaux / nombre total de personnes				
	Nombre de tentatives d'intrusions enregistrées / nombre total d'accès				
	Nombre de badges perdus ou oubliés sur la période				
03C	**Contrôle d'accès aux locaux sensibles**				
	Les indicateurs doivent refléter l'évolution de la sécurité des locaux sensibles				
	Nombre de personnes externes à l'entreprise ayant le droit d'accès aux locaux sensibles / nombre total des personnes (internes + externes)				
	Nombre d'intrusions détectées au cours de la période				
	Nombre d'équipements disparus (ou volés) / nombre total d'équipements (par catégorie d'équipements)				
03D	**Contrôle d'accès aux bureaux**				
	Les indicateurs doivent refléter l'évolution de la sécurité des bureaux				
	Nombre de personnes externes à l'entreprise ayant le droit d'accès aux bureaux / nombre total des personnes travaillant dans l'entreprise (internes + externes)				
O3E	**Sécurité contre les dégâts des eaux**				
	Les indicateurs doivent refléter l'évolution de la réactivité en cas d'inondation ou de dégâts des eaux				
	Temps d'évacuation des eaux au cours de la période				
	Fréquence de contrôle des systèmes de détection et d'évacuation				
	Nombre de détecteur d'humidité / surface des locaux considérés				
	Nombre de fausses alertes / nombre total d'alertes au cours de la période				
O3F	**Sécurité incendie**				
	Les indicateurs doivent refléter l'évolution de la réactivité en cas d'incendie				
	Nombre d'extincteurs par local / surface du local considéré				
	Nombre de détecteur d'incendie par local / surface du local considéré				
	Nombre de personnes formées à la sécurité incendie / nombre total de services (ou fonctions) de l'entreprise				
	Nombre total d'extincteurs de catégories différentes / Nombre total d'extincteurs installés				

2.4 Sécurité des architectures réseaux et télécommunications

Services		Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
04A	**contrôle d'accès aux réseaux**				
	Les indicateurs doivent refléter l'évolution de la qualité du contrôle d'accès aux réseaux				
	Nombre des interventions de télémaintenance / nombre total d'interventions				
	Nombre d'accès refusé / nombre total d'accès au réseau				
	Nombre d'accès refusés analysé par types de composants du réseau (firewall, routeur, systèmes d'authentification de type Radius, Tacacs)				
04B	**contrôle de la confidentialité des échanges et des communications**				
	Les indicateurs doivent refléter l'évolution de la qualité du contrôle de la confidentialité et des communications				
	pourcentage de messages avec chiffrement				
04C	**contrôle de l'intégrité des échanges et des communications**				
	Les indicateurs doivent refléter l'évolution de la qualité du contrôle de l'intégrité des échanges et des communications				
	pourcentage de messages avec signature				
04E	**intégrité des éléments de base du réseau**				
	Les indicateurs doivent refléter l'évolution de la qualité de l'intégrité des éléments de base du réseau				
	date de dernière mise à jour du plan de cablage				
	nombre de personnes autorisées à modifier le plan de cablage				
04F	**Intégrité du système d'adressage physique du réseau**				
	Les indicateurs doivent refléter l'évolution de la qualité de l'intégrité du sytème d'adressage physique du réseau				
	nombre de modification du plan d'adressage sur une période donnée				
	date de derniere mise à jour du plan d'adressage				
	date de la dernière sauvegarde				
04G	**protection de l'adressage physique**				
	Les indicateurs doivent refléter l'évolution de la qualité de la protection de l'adressage physique du réseau				
	date du dernier contrôle du fichier "log" du Firewall ou des routeurs.				
	nombre d'incidents relevés				
04H	**Sécurisation de l'administration réseau**				
	Les indicateurs doivent refléter l'évolution de la qualité de l'administration du réseau				
	nombre de personnes habilité à mettre à jour les autorisations				
04I	**Imputabilité des accès**				
	Les indicateurs doivent refléter l'évolution de la qualité de l'imputabilité des accès				
	fréquence des audits				
	date du dernier contrôle des accès				
	date du dernier contrôle des habilitations des administrateurs				
04J	**audit réseau**				
	Les indicateurs doivent refléter l'évolution de la qualité du respect des règles de sécurité définies				
	fréquence des audits				
	date du dernier audit				

2.5 Exploitation des réseaux et télécommunications

	Services	Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
05A	**Sécurité des procédures d'exploitation**				
	Les indicateurs doivent refléter la qualité du service rendu par l'exploitation des réseaux et des télécommunications (surtout si celle-ci est externalisée)				
	Nombre de contrats de service existants / nombre total de services fournis				
	Taux de couverture par service au cours de la période				
	Taux d'utilisation par ressource au cours de la période				
	Nombre de personnes ayant le privilège de plus haut niveau				
	Nombre de personnes ayant accès aux procédures cataloguées				
	Nombre de procédures cataloguées modifiées au cours de la période				
	Nombre d'activation des utilitaires sensibles au cours de la période				
	Date du dernier Contrat de maintenance avec les opérateurs de télécoms				
	Nombre de tentatives d'accès aux informations sensibles au cours de la période				
	Nombre d'activation de la télémaintenance au cours de la période				
	Nombre de modifications de la liste des personnes habilitées à accéder à l'administration au cours de la période				
05B	**Contrôle des configurations matérielles et logicielles**				
	Les indicateurs doivent refléter l'évolution de la protection des logiciels et matériels				
	Nombre de modifications des configurations au cours de la période				
	Dates des dernières versions de générations archivées				
	Nombre de modifications des sceaux de scellement au cours de la période				
	Nombre de vérifications de scellement effectuées au cours de la période				
	Nombre de configurations non conforme aux standards au cours de la période par type d'équipements				

	Services	Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
05C	**Continuité de fonctionnement**				
	Les indicateurs doivent refléter de la qualité de fonctionnement du réseau				
	Nombre de contrats de maintenance / nombre total de matériels en service				
	Nombre de contrats de maintenance des matériels sensibles / nombre total de matériels sensibles en service				
	Nombre de contrats de maintenance des logiciels sensibles / nombre total de logiciels sensibles en service				
	Nombre de maintenances effectuées au cours de la période				
	Nombre de dépassement de l'engagement de service de maintenance au cours de la période				
	Nombre d'arrêt du service réseau au cours de la période				
	Temps moyen d'arrêt du réseau au cours de la période				
	Temps cumulé d'arrêt du réseau au cours de la période				
	Nombre de modules de maintenance reçus du constructeur au cours de la période				
	Nombre de déclenchements du plan de reprise réseau au cours de la période				
	Nombre de sauvegardes réalisées au cours de la période				
	Pourcentage de logiciels essentiels sauvegardés au cours de la période				
	Taux de disponibilité du réseau				
	Nombre de tests du réseau de secours par an				
	Pourcentage de l'efficacité du plan de secours				
05D	**Contrôle, détection et traitement des incidents**				
	Les indicateurs doivent refléter le suivi de gestion des incidents				
	Pourcentage de résolution d'incidents au cours de la période par type d'incidents (matériel, logiciel, services réseaux, etc.)				
	Nombre de déclenchements des sondes réseaux au cours de la période				
	Nombre de paquets contenant des attributs de signature non valides au cours de la période				

2.6 Sécurité des systèmes et de leur architecture

	Services	Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
06A	**Contrôle d'accès aux systèmes et applications**				
	Les indicateurs pertinents permettront de renseigner sur l'utilisation des systèmes				
	Nombre de refus d'accès aux systèmes / Nombre total d'accès (aux systèmes) pour une période donnée				
	Nombre des accèdants par profil à un système choisi pour une période donnée				
	Nombre de traces révélant une attaque réussie / Nombre de traces de refus				
	Nombre d'accès constatés par profil en dehors des plages horaires pour une période donnée				
	Nombre de réclamations (pour des problèmes d'accès) auprès du helpdesk pour une période donnée				
	Nombre de virus détectés pour une période donnée				
	Nombre de tentatives de violation sur les environnements distants / Nombre d'environnements distants				
	Nombre de mots de passe crackés par un logiciel cracker / Nombre d'utilisateurs				
	Nombre de multiconnexions pour un même utilisateur sur une période donnée				
	Nombre d'accès administrateurs / Nombre d'utilisateurs				
06B	**Confinement des environnements**				
	Les indicateurs permettront de vérifier le cloisonnement (ou étanchéité) des différents environnements (production, exploitation, développement, test, essais, etc.)				
	Nombre d'utilisateurs ayant un accès autorisé "multi-environnements" / Nombre total d'utilisateurs				
	Nombre de passerelles entre environnement / Nombre d'environnement différents (production, exploitation, développement, test, etc.)				
	Nombre de supports remis à zéros binaire (ou détruits physiquement) / Nombre total de supports mis au rebut et contenant des informations sensibles ou nominatives				
06C	**Gestion et enregistrements des traces**				
	Les indicateurs doivent permettre de surveiller les évènements anormaux au niveau de la gestion et de l'enregistrement des traces				
	Nombre d'accès supprimés / Nombre de personnes ayant quitté l'entreprise pour une période donnée				
	Nombre de profils modifiés / Nombre de mutatuon et/ou changement de fonction				
	Pourcentage de mots de passe crackés / Nombre total de mots de passe déclarés				
	Nombre de fichiers infectés / Nombre de fichiés modifiés sur une période donnée				
	Nombre d'incidents graves / Nombre d'incidents enregistrés au niveau système				

2.7 Production Informatique

Services		Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
07A	**Sécurité des procédures d'exploitation**				
	Les indicateurs doivent refléter la sécurité des procédures d'exploitation, ils mesuront par exemple :				
	Nombre d'applications accompagnées de procédure(s) de mise en production / nombre total d'applications				
	Nombre d'applications mises en production au cours de la période				
	Nombre d'applications documentées / nombre total d'application en production				
	Nombre de procédures cataloguées modifiées au cours de la période				
	Nombre d'activation des utilitaires sensibles au cours de la période				
	Nombre et gravité d'incidents liés aux procédures d'exploitation.				
	Nombre de disparition et/ou de vol de documents imprimés.				
	Droits et/ou privilèges du personnel d'exploitation (Nombre + droits / nombre d'utilisateurs)				
07B	**Contrôle des configurations matérielles et logicielles**				
	Les indicateurs doivent refléter le contrôle des configurations matérielles et logicielles, ils mesuront par exemple :				
	Nombre de contrôles effectués au cours de la période / nombre d'incidents liés aux configurations matérielles et logicielles.				
	Nombre de logiciels modifiés / Nombre total de logiciels				
	Nombre de matériels modifiés / Nombre total des matériels				
	Quand a été effectué le dernier contrôle des licences de logiciels / progiciels				
	Quand a été effectué le dernier contrôle et/ou inventaire du matériel				
07C	**Gestion des supports de données et de programmes**				
	Les indicateurs doivent refléter la gestion des supports de données et de programmes, ils mesuront par exemple :				
	Nombre de programmes modifiés / Nombre total de programmes				
	Nombre de supports réalisés au cours de la période / Nombre d'incidents liés aux supports de données et de programmes.				
	Nombre personnes ayant accès aux locaux (sauvegardes & archivages / Nombre de personnes du département production informatique.				
	% de supports chiffrés / supports à risques ou critiques pour l'entreprise.				
	Nombre de disparition et/ou de vol de supports de données et de programmes.				
	Nombre de déclaration de disparition et/ou de vol de supports de données et de programmes statégiques.				

	Services	Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
07D	**Continuité de fonctionnement**				
	Les indicateurs doivent refléter la continuité de fonctionnement, ils mesuront par exemple :				
	Nombre de jours d'intervention de la maintenance au cours de la période / nombre de sites impliqués				
	Nombre de jours d'intervention de la télé-maintenance au cours de la période / nombre de sites impliqués				
	Taux de disponibilité des serveurs				
	% de sauvegardes testées au cours de la période / volume total des sauvegardes / nombre problèmes constatés				
	% d'applications et/ou de système critiques pour l'entreprise avec plan de secours opérationnel				
	Nombre de situations bloquantes ayant pour origine une défaillance matérielle ou logicielle				
	Nombre de situations bloquantes ayant pour origine une action du personnel de la production informatique				
	Nombre de situations bloquantes ayant pour origine une action du personnel du développement				
	Nombre de situations bloquantes ayant pour origine une action du personnel du support technique				
	Nombre de situations bloquantes ayant pour origine une action d'un utilisateur				
	Temps de tolérance face à une interruption d'une tâche vitale.				
	Taux de satisfaction du plan de reprise mis en place suite à incidents				
	Taux de satisfaction de la production informatique.				
	Taux de satisfaction du temps de réponse des ressources de la production informatique.				
	Nombre d'attaques virales au cours de la période pour les serveurs, les messageries, les postes de travail				
	% du Temps d'indisponibilité liée aux attaques virales / Temps total d'indisponibilité de l'exploitation des ressources au cours de la période.				
07E	**Gestion et traitement des incidents (erreurs, anomalies,…)**				
	Les indicateurs doivent refléter la gestionet traitements des incidents (erreurs, anomalies, ...), ils mesuront par exemple :				
	Nombre d'incidents au cours de la période / durée moyenne de traitement / durée la plus longue de traitement.				
	Nombre d'incidents résolus lors de la détection, de l'enregistrement, à l'appel de l'utilisateurs				
	Nombre d'incidents résolus dans un délai < 48 Heures				
	Nombre d'incidents non résolus après un délai de 5 jours				
	Nombre de contrôles effectués au cours de la période / nombre d'incidents relevés.				
	Nombre d'investigations sur incidents ou anomalies non terminées au cours de la période				
	Nombre d'incidents ayant la même origine au cours des 6 derniers mois.				

2.8 Sécurité applicative

Services		Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
08A	**Contrôle d'accès applicatif**				
	Les indicateurs pertinents permettront de renseigner sur l'utilisation des applications				
	Nombre de "propriétaires" d'applications / Nombre total d'applications				
	Nombre de personnes habilitées à changer les règles et autorisations d'une application choisie / Nombre de profils attribués à cette application choisie				
	Nombre de refus d'accès aux applications critiques et/ou sensibles / Nombre total d'accès (aux applications critiques et/ou sensibles) pour une période donnée				
	Nombre des accèdants par profil à une application choisie pour une période donnée				
	Nombre de traces révélant une attaque réussie / Nombre de traces de refus				
	Nombre de profils associés à des crénaux horaires et calendaires de travail / Nombre total de profils				
	Nombre d'accès constatés par profil en dehors des plages horaires pour une période donnée à une application choisie				
	Nombre de demande d'interventions auprès du helpdesk pour une période donnée sur une application choisie				
	Nombre de tentatives de violation sur les applications distantes / Nombre d'applications distantes				
	Nombre de mots de passe crackés (au niveau applicatif) par un logiciel cracker / Nombre d'utilisateurs				
	Nombre de multiconnexions (sur les applications critiques ou sensibles) pour un même utilisateur sur une période donnée / Nombre total d'applications critiques et/ou sensibles				
	Nombre d'accès "expert users" / Nombre d'utilisateurs				
08B	**Contrôle de l'intégrité des données**				
	Les indicateurs pertinents mesureront la qualité de l'intégrité des données confiées au Système d'Information.				
	Nombre d'incidents relevés au cours de la période				
	Nombre d'applicatifs scellés électroniquement / Nombre total d'applicatifs				
	Nombre non conformité des sceaux des applicatifs scellés sur la période				
	Nombre de modifications de programmes, en exploitation, contenant des contrôles / Nombre total de programmes contenant des contrôles				
	Par applicatif choisi :				
	Nombre de contrôles réalisés par l'utilisateur / Nombre de contrôles informatiques au cours de la période				
	Nombre de résultats différents entre les contrôles utilisateurs et les contrôles informatiques au cours de la période				
	Nombre de relectures incorrectes à partir de supports de sauvegarde ou d'archivage au cours de la période				
	Nombre de restaurations effectuées (par l'informatique ou à la demande de l'utilisateur) au cours de la période				
08C	**Contrôle de la confidentialité des données**				
	Les indicateurs pertinents mesureront la qualité de la confidentialité et leur risque de perte.				
	Nombre de refus d'accès aux applications critiques et/ou sensibles / Nombre total d'accès aux applications critiques et/ou sensibles pour une période donnée				
	Nombre d'applications chiffrées stockées / Nombre d'applications sensibles et/ou critiques				
	Nombre d'applications chiffrées transmises / Nombre d'applications sensibles et/ou critiques				
	Nombre de supports (sauvegarde et archivage) manquant à l'inventaire au cours de la période				
	Nombre de clés périmées ou interdites / Nombre total de clés actives				

Services		Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
08D	**Contrôle de la disponibilité des données**				
	Les indicateurs mesureront l'évolution de la disponibilité des données				
	Taux d'indisponibilité au cours de la période par applicatif sensible et/ ou critique				
	Nombre d'incidents de reconstitution de données ou de traitements sur la période				
	Temps moyen d'attente entre une demande de restauration de fichiers en exploitation (fichiers de données ou programmes) faite à l'exploitation et la disponibilité effective du (ou des) fichier(s) concerné(s)				
	Temps moyen d'attente entre une demande de restauration de fichiers archivés (fichiers de données ou programmes) faite à l'exploitation et la disponibilité effective du (ou des) fichier(s) concerné(s)				
	Temps moyen d'attente entre une demande de modification de fichiers (fichiers de données ou programmes) faite à la maintenance applicative et la disponibilité effective du (ou des) fichier(s) concerné(s)				
08E	**Continuité de fonctionnement**				
	Les indicateurs mesureront l'évolution de la continuité des traitements				
	Pour les traitements exigeant une disponibilité élévée, nombre de fois où les moyens redondants (unité centrale, fichiers miroirs) ont été sollicités au cours de la période				
	Nombre de versions de référence archivées en lieu sûr / Nombre d'applications en service				
	Nombre de procédures de reprise mise en route après un incident d'exploitation au cours de la période				
	Nombre de Plans de Continuité Utilisateurs (PCU) / Nombre total d'activités critiques de l'entreprise				
	Nombre de mises à jour effectives de Plans de Continuité Utilisateurs (PCU) au cours de la période				
	Nombre de mises à jour effectives de Plans de Continuité Utilisateurs (PCU) / Nombre d'activités critiques modifiées de l'entreprise				
	Nombre de tests effectifs de Plans de Continuité Utilisateurs (PCU) au cours de la période				
O8F	**Contrôle de l'émission et de la réception de données**				
	Les indicateurs mesureront l'évolution de la qualité des transactions automatisées				
	Nombre d'Accusé - Réception adressés / Nombre de transmissions sensibles				
	Nombre d'accusés de réception non reçus sur la période				

2.9 Sécurité des projets et développements

Services		Valeurs			
		Cible	Réelles au jj/mm/aa	Seuil mini	Seuil maxi
09A	**Sécurité des projets et développements applicatifs**				
	Les indicateurs doivent refléter la sensibilité de l'équipe de développement, la disponibilité des ressources, la traçabilité et fiabilité de l'application etc.				
	% de projets stratégiques incluant les critères DICT dans le cahier des charges				
	Taux de disponibilité des ressources (personnel de dev, support, exploit..)				
	Dernière date d'audit des critères DICT mesurables du projet				
	Niveau des critères DICT par rapport aux objectifs de sécurité visés				
	Dernière date d'audit du code et tests de l'application par une équipe indépendante				
	% du développement applicatif sous-traité				
	% de modules stratégiques dans l'application				
	% de modules stratégiques sous-traités				
	% de sous-traitants développant les modules stratégiques de l'application				
	Taux de renouvellement du personnel de développement des applicatifs stratégiques				
	Dernière date d'audit de la mise à jour de la documentation de l'application				
	Taux de révisions logicielles liées à des dysfonctionnements				
	Taux de documentations mises à jours par rapport aux applications supportées				
09B	**Organisation de la maintenance du logiciel applicatif**				
	Les indicateurs doivent refléter la compétence de la maintenance, sa fiabilité, sa capacité d'adaptation, sa rapidité d'intervention etc.				
	Taux de satisfaction des utilisateurs sur les interventions de la tiers maintenance				
	Dernière date d'audit de la procédure d'intervention rapide pour corriger les défauts de sécurité				
	Dernière date d'audit de la procédure d'intervention rapide pour corriger les défauts fonctionnels				
	Dernière date d'audit de la procédure d'intervention rapide pour corriger les défauts liés aux obligations légales				
	% d'applications haute disponibilité en dépassement de la capacité de disponibilité du SI				
	Taux d'interventions hors contrat de maintenance réalisés gratuitement				
	Taux d'incidents résolus référencés dans la base d'incidents du support applicatif				
	% de codes sources déposés par rapport aux produits maintenus				
	Dernière date d'audit du contrôle d'accès à la maintenance applicative				
09C	**Sécurité de la maintenance applicative**				
	Les indicateurs doivent refléter la compétence de la maintenance, sa fiabilité, sa capacité d'adaptation, sa rapidité d'intervention les compétences de l'équipe, etc.				
	Dernière date d'audit du contrat de support applicatif				
	Taux de satisfaction des utilisateurs de la maintenance applicative				
	% d'appels non résolus liés à un problème applicatif				
	Dernière date d'audit des tests de l'application par une équipe indépendante				
	Dernière date d'audit de la mise à jour de la documentation de maintenance de l'application				
	Nombre de maintenance à chaud pendant la dernière période				